ACEEE *Proc. of Int. Conf.* on *Recent Trends in Information, Telecommunication and Computing, ITC*

DNA based Password Authentication Scheme using Hyperelliptic Curve Cryptography for Smart Card

Vijayakumar P[1], Vijayalakshmi V[2] and Zayaraz G[2]
[1] Research Scholar, Dept., of ECE, Pondicherry Engineering College, Pondicherry, India
[1]Vijayrgcet@gmail.com
[2] Assistant Professor, Dept., of ECE, Pondicherry Engineering College, Pondicherry, India
[3] Associate Professor, Dept., of ECE, Pondicherry Engineering College, Pondicherry, India
Email: {[2]vvijizai@pec.edu,[3]gzayaraz@pec.edu}

***Abstract*— Smart Card technology is the emerging technology which is developing among common masses in our culture and widely used in the sectors of banking and industries. Many research works are undergoing in this area to provide highly confidential data transmission. Existing Scheme provides a security against offline attack for the lost Smart Card using Elliptic Curve Cryptography (ECC) but it requires more communication and computation overhead with higher key length. To overcome this limitation, DNA based Password authentication using Hyper Elliptic Curve Cryptography (HECC) scheme is proposed. It provides more security than existing system which allows server and smartcard to exchange the generated password and verify each other. This system exploits the advantages of Hyperelliptic Curve Cryptography (HECC) technique which is having lesser key size, less communication and computation overhead for Password generation and signature verification process.**

***Index Terms*— Smartcard, Hyper Elliptic Curve Cryptography, Deoxyribo Nucleic Acid, Communication complexity Computational complexity, Password generation, Authentication, Elliptic Curve Cryptography.**

I. INTRODUCTION

Smart cards are widely used in many business systems which provide portable benefits and secure data storage, and it also incorporated in many computing systems. Smart cards are provided with memory card which can enable to store and secure the information using available cryptographic algorithm. Deoxyribo Nucleic Acid (DNA) based computing technology combined with cryptographic algorithm will provide secure authentication for smartcard. DNA is a long linear polymer found in the core part of a cell. DNA is made up of several nucleotides in the form of double helix and it is linked with the transmission of genetic information. DNA based computing technique mainly focuses on storage capacity and its unique property. Hyperelliptic Curve Cryptosystem (HECC) is used in many power constrained devices which offer equal security as any other public key cryptosystem with much smaller key length. This cryptographic system allows highly efficient computation of the underlying field arithmetic. Hyperelliptic Curve Cryptosystem is very much popular among other cryptosystems such as Elliptic Curve Cryptosystem (ECC), Rivest Shamir Adleman (RSA), Digital Encryption Standard (DES), etc., due to its shorter key length [1-5]. This section gives the introduction about smart card, DNA and Hyperelliptic Curve Cryptography. Section II describes related works. Section III deals with different phases for providing robust password authentication scheme

DOI: 02.ITC.2014.5.581

using ECC. Section IV briefly explains mathematical background of Hyperelliptic Curve Cryptography and also explains DNA based password authentication scheme using HECC. Section V deals with results and discussion in this context. Finally, it concludes the paper.

II. Related Works

Xing Wang applied DNA computing theories for cryptography security which transmits the message securely and effectively. This paper shows how cryptography works with DNA computing technique. Here, most famous asymmetric key RSA algorithm is used to encrypt the message and decrypt the message to provide greater level of security with 1024 bit key size. Major drawback of this algorithm is increased key size tends to increased computational complexity [6]. Reference [7] propose a novel DNA based Elliptic Curve Cryptography algorithm which provide the same level of security as [6] with lesser key size by employ the advantage of ECC. As a result, it gives lesser communication and computation overhead. Guozhen Xiao [8] pointed out the biological background of DNA cryptography and principle of DNA computing. This paper compares the status, security and application fields of DNA cryptography with traditional cryptography and quantum cryptography. Guangzhao Cui [9] provides information about background principle of DNA computing, challenges behind DNA computing based cryptology, DNA encryption techniques and application of DNA Computing security field. It gives brief introduction about DNA steganography and DNA authentication. Wen-Bing Horng [10] offers a secure and efficient user authentication scheme for smart card which will improve the level of security of the Peyravian-Zunic scheme. He also reveals the weakness of Kwon et al.'s protocol concerning off-line password forgery attack and guessing attack. Xiaoyi-Ying [11] proposed a novel key authentication scheme which combines the fuzzy extractor concept with Smart Card. This scheme can avoid guessing attack, parallel attack and masquerade attack. Seoul [12] uses symmetric key cryptosystem with modular exponentiation to make an efficient authentication scheme for non-tamper resistant smart card. He showed that Song's scheme is weak to the offline password guessing attack and the insider attack. Nenghai Yu [13] proposed a secure scheme which is very efficient, both in term of computational complexity and storage capacity. This scheme is very suitable for providing remote authentication in distributed application and also it was developed against password guessing attack, masquerade attack and replay attack. Roy prevents the clogging attack by implementing two party identity-based authenticated key agreement protocols [14].

III. Existing Password Authentication Scheme

Existing password authentication scheme for smart card consists of five phases: Parameter generation phase, registration phase, pre-computation phase, login phase and password changing phase. In parameter generation phase, server generates a large prime number, two field elements. With the help of these number fields, it will generate a point from order n. Server also selects private key and public key for exchanging a data between the users and distributes the generated parameter. In registration phase, user uses the Smart card to send identification information to server for authentication purpose. The user receives and stores the parameter into the smart card. In Pre-computation phase, smart card generates a random variable and stores the calculated values in a card memory for further use. In log-in phase, session key is generated, verified and exchanged between user and Smart Card. In password changing phase, user can able to change the password frequently with the help of session key which is produced in log-in phase [15].

IV. Proposed Dna Based Password Authentication Scheme Using Hyperelliptic Curve Cryptography

Existing scheme needs to enter the password directly which will create insecure environment between smart card and server. It exploits the advantages of Elliptic Curve Cryptography for key exchange, encryption and decryption process. It require 160 bit key length to provide greater level of security, tends to high communication and computational overhead. In order to avoid the above limits, DNA based password authentication scheme using Hyperelliptic Curve Cryptography is proposed. This will generate the password based on DNA molecule and will authenticate both smart card and server. In order to provide higher level of security, password generation phase and authentication phase is added in this proposed scheme. The proposed scheme employs the advantages of Hyperelliptic Curve Cryptography to provide same level of security with 80-bit key size, and less communication and computational overhead. In 1988, Neal Koblitz

proposed an expansion of Elliptic Curve cryptosystem known as Hyperelliptic Curve Cryptosystem. Hyperelliptic Curve Cryptosystem was widely used fast public key cryptosystem in many power constrained devices with high efficiency and security. HECC was very much famous because of its high efficiency, shorter key length, easily implemented for software and hardware applications, less communication and computational overhead, less consuming power, less processing time. The security of HECC is based on the Hyperelliptic Curve Discrete Logarithmic Problem (HECDLP), (i.e) k ε Zp, the computation of K=k × P where K is the private key and P is the public key of the user. So, the security of HECC lies on the discrete logarithm problem in the Jacobian of the curve [16-20]. These security features and characterize of HECC allows to use in less memory and less power smart card device. Hyperelliptic points are generated from the curve C which form a Jacobian group and divisor. These two key elements are useful for cryptographic scheme which is transformed from Hyperelliptic Curve. Proposed scheme enhances the server performance when Smart card content is disclosed. Proposed scheme consists of six phases: Parameter generation phase, Password generation phase, Registration phase, Pre-Computation phase, Authentication phase and Password changing phase.

A. Parameter Generation Phase

The related parameters are generated using Hyperelliptic Curve C for encryption and decryption process. From the curve C, private and public keys are generated using contor algorithm. The process involved to generate both keys is shown as follows:

Input : Public parameters are Hyperelliptic curve C, prime p and divisor D.
Output : Public key Ps and Private key Xs.
Process :
Step 1: Server choose a Hyperelliptic curve Equation of genus g (g >2) over F(q) as shown in (1)

$$y^2+h(x).y=f(x) \qquad (1)$$

where,
h(x) is a polynomial of degree, g.
f(x) is monic polynomial of degree 2g+1, which satisfies the equation ,

$$h(x)' \,.\, y = f(x) \qquad (2)$$

$$2y + h(x) = 0 \qquad (3)$$

Step 2 : From the points of Hyperelliptic curve C, server generates a set of elements of Jacobian over $J(F_q)$ can be represented in (4),

$$D = \sum m_i P_i \qquad (4)$$

where

$m_i \geq 0$
D - Reduced divisor
P_i - Finite points

Step 3: The server generates a point G from order n, satisfies n x G=0.
Step 4: The server picks a random number X_s to be the private key and computes the public key $P_s=X_s$ x G.
Step 5: The server issues the parameter (P_s, G, D, C, n).

B. Password Generation Phase

Each user receives the parameter before joining into the network, which is provided by server. Instead of giving password directly, password is mapped with DNA molecule along with the number to provide greater level of security which is not known to the eavesdropper who always tries to retrieve the password. Password is generated by combining DNA molecules such as Adenine (A), Thymine (T), Guanine (G) and Cytosine(C) as shown in Table II.

Step 1: Server can map the password message with DNA nucleotide using the Table I.
Step 2: Convert the DNA nucleotide into number using the Table II.
Example
Password : Hyper
DNA standard : ATG AAA ACA TTT ACT
Password : 104030 101010 102010 404040 102040

TABLE I. CONVERSION OF PLAIN TEXT TO DNA MOLECULE

A - CCA	K - GAA	U - GTC
B - GTT	L - CGT	V - TCC
C - TTG	M - CCT	W - GCC
D - GGT	N - TCT	X - ACT
E - TTT	O - CGG	Y - AAA
F - TCG	P - ACA	Z - TCA
G - CGC	Q - CAA	
H - ATG	R - ACT	
I - AGT	S - GCA	
J - CGA	T - CTT	

TABLE II. CONVERSION OF NUCLEOTIDE TO NUMBER

A -10	C -20	G -30	T -40

C. Registration Phase

The user can use the smart card to send identification information for the server to authenticate as shown in Figure.1.

Step 1: If the smart card wants to register at the server with its own identity (ID_i) and password (PW_i), user has to compute the password as shown in the above example and send it with username to the server over a secure channel. Smart card chooses a random number RN_1, Identity ID_i and calculates U_1 value using the generated password $F(PW_i)$ as shown in (5).

$$U_1=h(F(PW_i \oplus RN_1^{-1}). \quad (5)$$

Then smart card sends $\{ID_i, h(F(PW) \oplus RN_1, U_1)\}$ to the server.

$$\text{Smart Card} \longrightarrow \text{Server} : \{ ID_i, h(F(PW_i) \oplus RN_1, U_1)\} \quad (6)$$

Step 2: Server generates a random number S_1 as secret key and chooses another random number RN_2 and calculates U_2 value using U_1 and RN_2. Server also provides the expiry date (EDi) and time stamp (Tsi) for each user to check its validity and time period respectively as shown in (8).

$$U_2=U_1*RN_2^{-1} \quad (7)$$

$$Y_i= h(ED_i,Ts_i) \quad (8)$$

$$Q_i=E_{s1}(h(F(PW_i) \| RN_1) \| U_2 \| ID_i \| CI_i \| h(ID_i \| CI_i \| h(F(PW_i) \| RN_1 \| h(ED_i,Ts_i)) \quad (9)$$

$$V_i=h(ID_i,S_1,CI_i) \quad (10)$$

Smart Card memory consists of following parameters

$$e = r *G \quad (11)$$

$$c = r * P_s = r * x * G \quad (12)$$

Then, server issues certificate to user i that contain the parameters (IDi,CIi,Qi,Vi,Yi).

Step 3: User receives these information (IDi,CIi,Qi,Vi,Yi) and stores into the smart card.

D. Pre- Computation phase

Smart card chooses a random number r and calculates e=(r*G) and c=(r*P_s)=r*x*G. Then (e,c) is stored in card memory for use in the authentication phase.

E. Authentication Phase

If user i log-in to the server by using his own smart card content and respective password as shown in Figure.2.

Step 1: Smart card calculates $Ev_i(e)$ and send $Ev_i(e)$ and Q_i to the server e=(r x G).

Step 2: Server uses secret key S_1 to decrypt $Q_i = (U_2 \| ID_i \| CI_i \| h(F(PW_i) \| RN1 \| h(EDi,Tsi)))$ and calculates,

$$U_1=U_2*RN_2 \quad (13)$$

$$Y_i=h((ED_i,Ts_i) \quad (14)$$
$$V_i= h(ID_i,Y_i,U_1,CI_i). \quad (15)$$

F. Mutual Authentication

The server will verify the parameter comparing with the calculated values

- Is CI_i is stored in the registration table
- Is ID_i in the registration
- Is Date is expired
- Is Time Stamp is equal

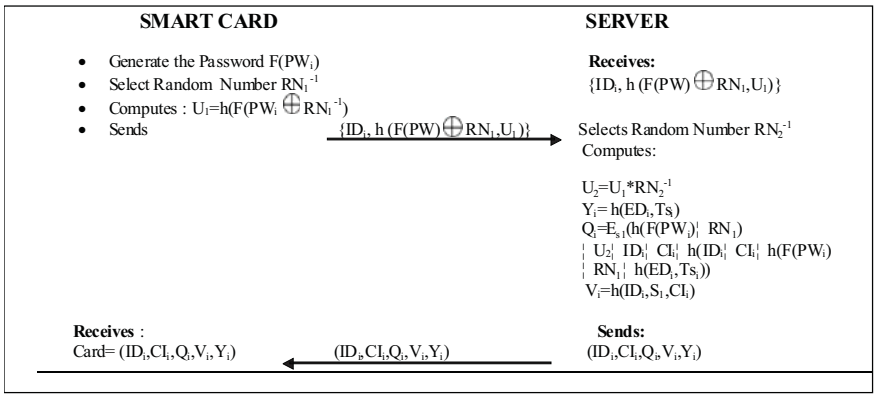

Figure 1. Registration Phase

If any of the above verification is false then server rejects the agreement. If above verifications are true, then the server selects the random number R_s and calculates,

$$c=e*x=r*x*G \quad (16)$$
$$M_s=h(c \parallel R_s \parallel V_i \parallel Y_i) \quad (17)$$

Server sends (c, M_s) to the smartcard

Step 3: Smart card calculates and checks M_s, then Smart Card send M_u to the server.

$$M_u=h(h(PW_i \parallel RN_1) \parallel U_1 \parallel c \parallel R_s) \quad (18)$$
$$S_k =h(V_i, c, u) \quad (19)$$

Step 4: Server checks Mu. If M_u is true, calculates session key S_k =h (V_i, c, u) accepts login request.

G. Password-Changing Phase

User 'i' wants to change password. Change the message using session key, can encrypt smart card. Session key is produced in authentication phase. Smart card selects a random number RN_1* and another new password $F(PW_i)$* and sends, Esk (ID_i,$h(F(PW_i)$* ‖ RN_1*)) to the server. Server receives the messages. It recalculates Q_i*, Q_i*=Es(h($F(PW_i)$* ‖ RN_1*) ‖ ID_i ‖ CI_i ‖ h(ID_i ‖ CI_i ‖ h($F(PW_i)$*‖RN_1*))). Sends Esk(Qi*) to smart card. Smart card will decrypt Qi* using session key and store in its memory.

V. Simulation Results And Discussions

The simulation parameters are processing time and key size: Processing time is the total time taken to finish the task (phase) by the personal computer. Key size is the size of the key used for encrypts and decrypt the message using HECC. MATLAB software is used to implement the proposed scheme which consists of parameter generation phase, password generating phase, registration phase, pre-computation phase, authentication phase, and password-changing phase. Simulation results show the variation of processing time of each and every phase with respect to the key size. From this result, it is inferred that the number of bits involved providing authentication using HECC is less than ECC. Finally, performances of both existing and proposed scheme are compared for each and every phase with respect to key size as show in table.3.

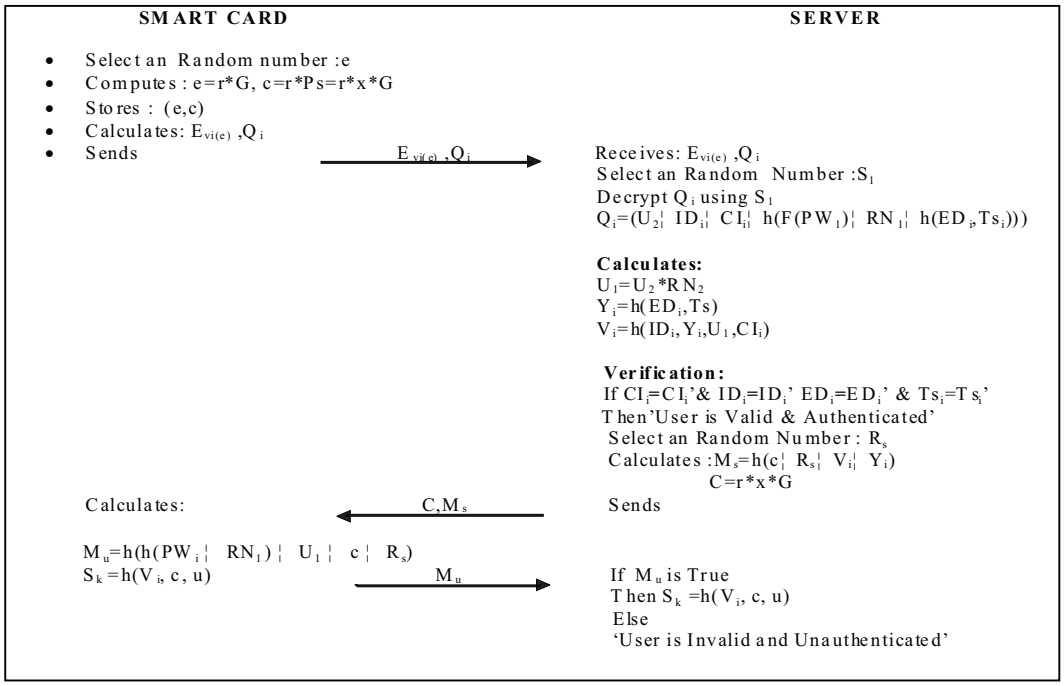

Figure 2. Authentication phase

Parameter generation phase took more processing time for generating parameters using existing scheme (ECC) than proposed scheme (HECC). From the Figure.3, it is inferred that for key size 35 bits, ECC takes the processing time of 389 milliseconds whereas HECC takes only 289 milliseconds. Figure.4 shows that the total time taken to map DNA molecule with password, and mapping of Nucleotide to number is 270 ms (52 bit key size). ECC takes the processing time of 320 milliseconds for the same key size. During registration process, user receives parameter from the trusted server, and stores it in smart card memory which takes processing time of 479ms for ECC, and 343ms for HECC (52 bit key size) as shown in Figure.5. Pre-Computation phase generates two parameter e and c which are used for mutual authentication phase take 250ms (ECC) and 198ms (HECC) for the same key size as shown in Figure.6. Figure.7 shows that total processing time taken to authenticate both server and smart card with the help of generated parameter for 52 bit key size. For the key size 52 bits, ECC takes the processing time of 512 milliseconds, whereas HECC takes only 353 milliseconds. User wants to change the password in password changing phase takes only 275ms for HECC and 510ms for ECC (35 bit key size) as shown in Figure.8.

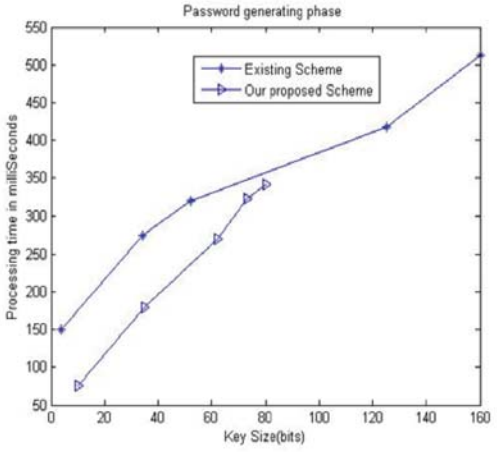

Figure 3. Parameter generation phase

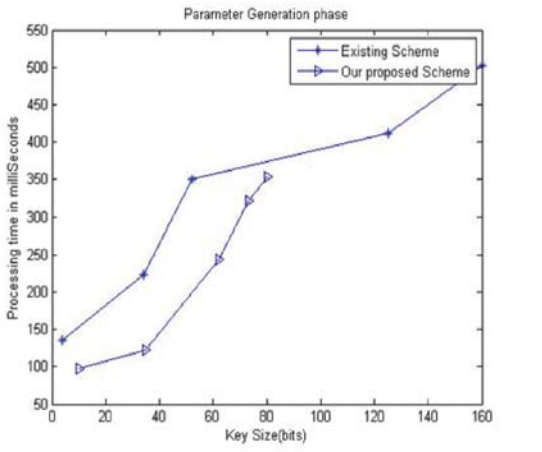

Figure 4. Password generating phase

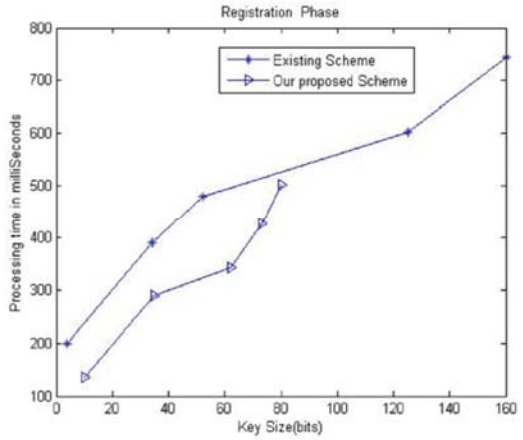

Figure 1. Registration phase

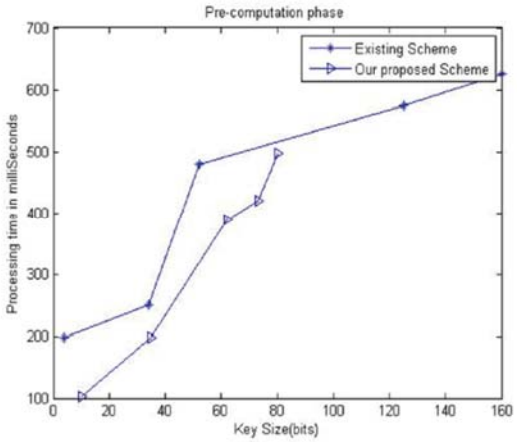

Figure 6. Pre-Computation phase

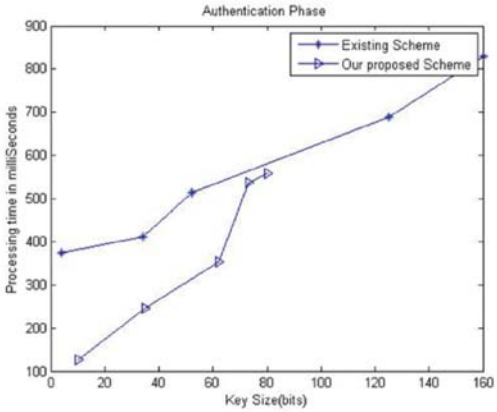

Figure 7. Authentication phase

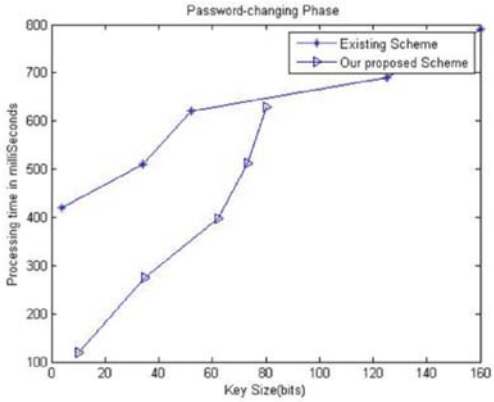

Figure 8. Password changing phase

TABLE III. COMPARISON TABLE

S.No	Phase	Existing Scheme		Proposed Scheme	
		Key size(bits)	Processing time(ms)	Key size(bits)	Processing time(ms)
1	Parameter Generation	52	350	52	243
2	Password Generating	52	320	52	270
3	Registration	52	479	52	343
4	Pre-computation	52	480	52	389
5	Authentication	52	512	52	353
6	Password-Changing	52	620	52	398

VI. CONCLUSION

Existing authenticated key agreement scheme fails to save the password from the eavesdroppers whereas DNA based password authentication scheme avoids password hacking by mapping original message with DNA molecule along with number to improve the level of security. Proposed scheme replaces ECC by extended cryptosystem for encryption and decryption of message which consumes less power and less processing time suitable for power constrained device. Addition of mutual authentication phase enables to check validity and identity of both user and server which avoid denial of service, non-repudiation, data integrity and forgery. Password changing phase avoid phishing and hacking of password.

REFERENCES

[1] Fritz W. and Hanka O., "Smart Card Based Security in Locator/Identifier – Split Architectures", in the IEEE proceedings of Ninth International Conference on Networks (ICN), pp.194 - 200, April 2010.

[2] Bochen Fu and Xianwei Zhang , "DNA cryptography based on DNA Fragment assembly", in the IEEE proceedings of 8th International Conference on Information Science and Digital Content Technology (ICIDT**),** vol.1, pp.179-182, June 2012

[3] Tutanescu I. Anton C. Ionescu L. and Caragata D. , "Elliptic Curves Cryptosystems approaches", in the IEEE proceedings of Information Society i-Society, pp.357 – 362, 2012.

[4] Kou Yingzhan , "Extended Fault Analysis on Elliptic Curve Cryptosystems against Repeated Doubling", in the IEEE proceedings of international conferences of Instrumentation, Measurement, Computer, Communication and Control, pp.545 – 548, 2011.

[5] Xinxin Fan, Thomas Wollinger, and Guang Gong," Efficient Explicit Formulae for Genus 3 Hyperelliptic Curve Cryptosystems", in the IEEE Journal proceedings of Information Security, vol.1 , Issue: 2 , pp.65-81, June 2007.

[6] Xing Wang and Qiang Zhang, "DNA computing-based cryptography", in the IEEE proceeding of Fourth International Conference on Bio-Inspired Computing, pp.1 – 3, Oct 2009.

[7] Vijayakumar P., Vijayalakshmi V. and Zayaraz G., "DNA Computing based Elliptic Curve Cryptography" in the International Journal of Computer Applications, vol.36, no.4 , pp.18-21, Dec.2011.

[8] Guozhen Xiao, Mingxin Lu, Lei Qin and Xuejia Lai , "New field of cryptography: DNA cryptography", in the Journal on Chinese Science Bulletin , vol.51, Issue 12 , pp.1413-1420, June 2006.

[9] Guangzhao Cui, Cuiling Li, Haobin Li and Xiaoguang Li, "DNA Computing and Its Application to Information Security Field", in the IEEE proceedings of Fifth International Conference on Natural Computation, pp.148-152, June 2007.

[10] Wen-Bing Horng , Cheng-Ping Lee and Jian-Wen Peng, "Security weaknesses of song's advanced smart card based password authentication protocol, in the IEEE proceedings of International Conference on Progress in Informatics and Computing (PIC), pp.477 - 480 , Dec. 2010.

[11] Xiaoyi Duan and XiuYing Li, "Security of a new password authentication scheme using fuzzy extractor with Smart Card", in the IEEE proceedings of 3rd International Conference on Communication Software and Networks (ICCSN), pp. 282 - 284,May 2011.

[12] Seoul .K, Seo .S and Choi Jin-Young , "Security analysis of smart card based password authentication schemes, in the IEEE proceedings of 3rd International Conference on Information Sciences and Interaction Sciences (ICIS), pp.352 - 356 ,June 2010.

[13] Zhuo Hao and Nenghai Yu , "A Security Enhanced Remote Password Authentication Scheme Using Smart Card", in the IEEE proceedings of International Symposium on Data, Privacy and E-Commerce (ISDPE), pp.56 – 60, 2010.

[14] Roy S., Das A.K. and Yu Li , "Cryptanalysis and security enhancement of an advanced authentication scheme using smart cards, and a key agreement scheme for two-party communication", in the IEEE proceedings of IEEE 30th International conference on Performance Computing and Communications Conference (IPCCC), pp.1 - 7, Nov. 2011.

[15] Wen-Chung Kuo, KaiChain, Jin-Chiou Cheng and Jar-Ferryang, "An Enhanced Robust and efficient Password Authenticated key agreement using smartcards", in the proceedings of International Journal of security and its applications, vol.2, pp.127- 132,2012.

[16] Avanzi R.M, and Tanja L., "Introduction to Public key cryptography from Handbook of Elliptic and Hyper Elliptic Curve cryptography", Henri Cohen, Gerhard Frey, Chapman and Hall/CRC, Taylor and Francis, Florida, 2006.

[17] Ganesan R., Mohan G. and Vivekanandan K., "A Novel Digital Envelope Approach for A Secure E-Commerce Channel", in the proceedings of International Journal of Network Security, vol.11, no.3, pp.121-127, Nov. 2010.

[18] Gaudry P. and Thome E., "A double large prime variation for small genus Hyper Elliptic index calculus", Cryptology ePrint Archive, Report 2004/153, 2004. Available at http://eprint.iacr.org/

[19] N. Boston, T. Clancy, Y. Liow, and J. Web-ster. Genus Two Hyperelliptic Curve Coprocessor. In CHES, NCS, New York, 2002. Springer Verlag.

[20] Gaudry P. and Thome E., "A double large prime variation for small genus Hyper Elliptic index calculus", Cryptology ePrint Archive, Report 2004/153, 2004. Available at http://eprint.iacr.org/

AUTHORS

P. Vijayakumar is currently working as Assistant Professor (Sr.) in School Electronic Science Engineering at VIT university Chennai campus, India and pursuing Ph.D in Pondicherry University. He completed his B.Tech in Rajiv Gandhi College of Engineering and Technology and M.Tech in Pondicherry Engineering College which is affiliated to Pondicherry University. He has 7 years of teaching experience. To his credit, he has published more than 15 research papers relating to Cryptography and Network Security in several National / International Journals and Conferences. He can be reached by email at vijayrgcet@gmail.com

Dr. V. Vijayalakshmi is currently working as Assistant Professor in Electronics & Communication Engineering Department at Pondicherry Engineering College, Puducherry, India. She completed her B.Tech, M.Tech and PhD in Pondicherry Engineering College which is affiliated to Pondicherry University. She has 20 years of teaching experience. To her credit, she has published more than 25 research papers relating to Network Security and software Engineering in several National / International Journals and Conferences. She can be reached by

Dr. G. Zayaraz is currently working as Professor in Computer Science & Engineering Department at Pondicherry Engineering College, Puducherry, India. He received his Bachelor`s, Master's and Doctorate degree in Computer Science & Engineering from Pondicherry University. He has published more than twenty five research papers in reputed International Journals and Conferences. His areas of specialization include Software Architecture and Information Security. He is a reviewer for several reputed International Journals and Conferences and Life Member of CSE, and ISTE. He can be reached by email at gzayaraz@pec.eduemail at vijizai@pec.edu